Email Attack: What it is, red flags to spot, and what to do if you clicked

Gridinsoft Help Center

What it is

An email attack uses your inbox as the doorway. Criminals send messages that trick you or deliver malware - from fake "account alerts" to booby-trapped invoices - aiming to steal logins, install spyware/ransomware, or get you to send money.

Common plays

- Phishing: look-alike logins grab your password.
- Malware attachments: invoices/ZIPs/scripts that infect your device.
- Business email compromise (BEC): "CEO/CFO" asks for urgent payment or gift cards.
- Link shorteners & look-alikes: buttons say one thing; URL goes elsewhere.

Red flags

- Urgent tone ("pay now," "verify in 15 minutes")
- Sender name looks right, address doesn’t
- Odd file types: .zip, .js, .exe, macro-enabled Office files
- Links that don’t match the real site when you hover

If you clicked

- Disconnect from the internet; don’t open banking/crypto.
- Scan with trusted anti-malware; reboot and scan again.
- From a clean device, change passwords and turn on MFA.
- In email settings, remove suspicious forwarding rules and sign out of other sessions.
- Tell IT/support and anyone who might be affected.

Prevent it

- MFA everywhere; a stolen password alone won’t work.
- Use a password manager and unique passwords.
- Preview links (hover/tap-and-hold) and don’t open unexpected attachments.
- Keep your device, browser, and mail app updated; enable spam/attachment filtering.
- For teams: add DMARC, DKIM, SPF and train staff to verify money/account changes out of band.